International Journal of Advancement in Engineering Technology, Management & Applied Science

Volume 3, Issue 6 June 2016 ISSN No: 2349-3224

IMMEDIATE EMERGENCY MESSAGE SCHEME FOR VEHICULAR ADHOC NETWORK

Ms. Pallavi Akulwar[1], Prof. Guraudev B. Sawarkar[2]

[1] *M.Tech Student, Department of Computer Science & Engineering*
VM Institute of Engineering and Technology, Nagpur

[2]*Associate Professor, Department of Computer Science & Engineering*
VM Institute of Engineering and Technology, Nagpur

Abstract*— *The many researches use the various kinds of the authentication scheme to secure the vehicular network on the basis of research road jamming is an ascending order due to an industrial research to find out of some solution to preserving this condition like most of technique is used to secure network but for the security they all method are failed to detect or finding out the attacks for the region the communication is not more secure for that purpose the aim of presented investigation propose system is to develop a secure vehicular authentication scheme in this paper we can used SUMO is technique to communicate message for that message security we can used ACO algorithm and with the help of DOS and DDOS vehicular network to increases the efficiency of transport as well as traffic safety in which through the wireless communication vehicle exchange information directly. The aim of presented investigation is to develop a secure vehicular authentication.

***Keywords*—** VANET, Protocols, Authentication privacy preserving scheme, Message jamming, SUMO, Emergency warning notification, Vehicular ad hoc network.

I. INTRODUCTION

Many research and scientific process require vehicular networking infrastructure for safety communication VNET reduce the risk of accident of vehicular to vehicular networking. Vehicular network is an ad-hoc network to enhancing comfort as well as safety road side traffic.VANET is recognised as well as important component for the intelligent system of transformation. The VANET in a used to improving safety and secure and efficiency of the transportation system. in this paper the propose system when jamming take place the sensor can be activate and they can send message to authorised section. and this message is an sending is secrete form and this message can read of the authorised section After then to find out the location and distance which the help of the longitude and latitude distance formulas. Then this distance and exact location can send to authorised section with the help of ACO technique. SMTP protocol is used to send the message to vehicular network .in the proposed system to overcome the problem of attack in network path the various kind of attacks are infected to secure communication of network but some time attacks may be very strong i.e. message will damages and not give some correct information in exact time domain for that reasons in the propose system to find out some solution of network attacking i.e. Sybil attacks, forgery attacks, Replay attacks, this all are attacks are finding out the existing system to overcome out of this problem to find the solution.

International Journal of Advancement in Engineering Technology, Management & Applied Science
Volume 3, Issue 6 June 2016 ISSN No: 2349-3224

Sybil attacks- Sybil attacks is type of security threats when a node in a network claims multiple identities most network like peer to peer network, relay on assumption of identity, where each computer represent one identity.

Forgery attack- Forgery attack attempts to forge on http request on behalf of on authenticated user by inserting a specially crafted scripting code forces on action on.

Replay attacks- Replay attacks are an attack capture message form Bob to Alice; later replay message to Alice.

Above all of this attacking to solve this problem of network conjunction. In this paper of proposed system Sybil attacks, forgery attacks, replay attacks are all the is on software attacks all as may attack on the VANET secure section i.e. for that the reason the information of this secure network is not go to secure form and not exact time i.e. this all issues of this software attacks to find out the solution of proposed system.

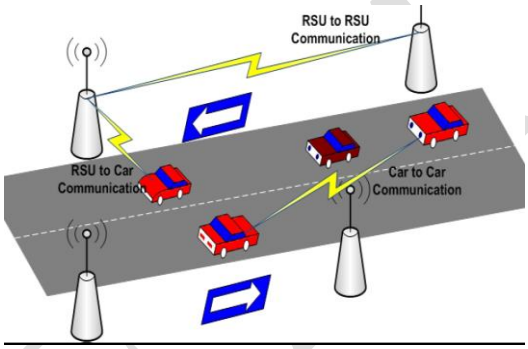

Fig 1 VANET Structure

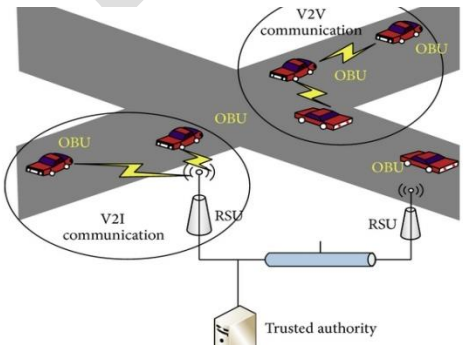

Fig 2 Designing of secure network

II Related work

(VANET) Vehicular ad hoc network is recognized as an important Component of Intelligent Transportation Systems. The main benefit of VANET communication is seen in active safety systems, which target to increase safety of passengers by exchanging warning messages between vehicles. To improve the safety, security and efficiency of the transportation systems

and enable new mobile applications and services for the traveling public, Intelligent Transportation Systems (ITS) have been developed, which apply rapidly emerging information technologies in vehicles and transportation infrastructures. Vehicular networking has significant potential to enable diverse applications associated with traffic safety, traffic efficiency and infotainment.

III PROPOSED SCHEME

In this paper to find the solution above on the software attacking section to overcome vehicular problem in network security section.VANET form very long time this VANET network work put not properly i.e. not give information in correct time.VANET consist the nodes of large range. VANET with the help of DSRC radio signals is a processing of communication. Short range using range of DSRC is as reach 1 KM. This communication is on the basis of adhoc form so that the no wires are required and connected node can freely move.

RSU- Road side unit is a router used working between vehicles on the road also connected to another network device.

OBU- Vehicular has contained on board unit this unit are connected vehicle with RSU via DSRC radio.

TPD- TPD is a unit this device transfer proof devices all secrets information about vehicle holding the TPD i.e. all the details information of vehicle.

CPP- CPP conditional privacy preserving and V2I communication provides an efficient batch verification process as means of optimizing the verification performance in V2I communication and conditional privacy preserving.

BAT- Binary Authentication Algorithm this algorithm is based on the BAT whose aim is to find the bogus signature in the signature.

IV CONCLUSION

VANET is a most promising AD Hoc vehicular network technology. VANET we will process to find new solution to secure the VANET network. VANET is ttacking issues in network communication. To helping the secure VANET network to overcomes security issues. The proposed research can be minimizing attack on vehicular ad hoc network. The proposed research can be minimizing attack on vehicular ad hoc network. System can encrypt and decrypt the text message easily without interrupt. The system can broadcast the short message to all in encrypted form but this broadcasting message can decrypted by the emergency vehicle in that region. No any vehicle can decrypt this message except emergency vehicle. For that system uses a cryptography technique. And in this way system can successfully transmit the message with secure network and secure channel.

ACKNOWLEDGMENT

In our system we find solution and to overcome the a(VANET) Vehicular ad hoc network is Recognized as an important Component of Intelligent Transportation Systems. The main benefit of VANET communication is seen in active safety systems, which target to increase safety of passengers by exchanging warning messages between vehicles. To improve the safety, security and efficiency of the transportation systems and enable new mobile applications and services for the traveling public, Intelligent Transportation Systems (ITS) have been developed, which apply rapidly emerging information technologies in vehicles and transportation infrastructures. Vehicular networking has significant potential to enable diverse applications associated with traffic safety, traffic efficiency and infotainment.

REFERENCES

[1] S. Srivisshudhanan "Analysis of QOS in WiMAX Networks" Periyar University Internationl Journal of Advancement in Engineering Technology, Management and Applied science,volume2.Issue 5 May 2015,ISSN No:2349-3224.

[2] Attila Altay Yavuz "An Efficient Real-Time Broadcast Authentication Scheme for Command and Control Messages" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 10, OCTOBER 2014.

[3] Neeraj Kumar and Jong-Hyouk Lee "Peer-to-Peer Cooperative Caching for Data Dissemination in Urban Vehicular Communications" IEEE SYSTEMS JOURNAL, VOL. 8, NO. 4, DECEMBER 2014.

[4] Vinh Hoa LA, Ana CAVALLI "Security Attacks And Solutions in vehicular Ad-hoc network" International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[5] Senthil Ganesh N. Ranjani S. "Security Threats on Vehicular Ad Hoc Networks (VANET)" International Journal of Electronics Communication and Computer Engineering Volume 4, Issue (6)NCRTCST-2013, ISSN 2249–071X.

[6] Kyung-Ah Shim "Reconstruction of a Secure Authentication Scheme for Vehicular Ad Hoc Networks Using a Binary Authentication Tree" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 11, NOVEMBER 2013.

[7] Agrawal, Aditi Garg, Niharika Chaudhiri, Shivanshu Gupta, Devesh Pandey, Tumpa Roy " Security on Vehicular Ad Hoc Networks (VANET)" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013).

[8] Rashmi Raiya,Shubham Gandhi "Survey of Various Security Techniques in VANET" Volume 4, Issue 6, June 2014 ISSN: 2277 128X.

[9] Mehdi Khabazian, Member, IEEE, Sonia Aïssa, Senior Member, IEEE, and Mustafa Mehmet-Ali, Member, IEEE "Performance Modeling of Safety Messages Broadcast in Vehicular Ad Hoc Networks" IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 14, NO. 1, MARCH 2013.

[10] Josiane Nzouonta, Neeraj Rajgure, Guiling Wang, Member, IEEE, and Cristian Borcea, Member, IEEE "VANET Routing on City Roads using Real-Time Vehicular Traffic Information" December 14, 2007; revised July 24, 2008 and December 23, 2008. This work is supported in part by the National Science Foundation under Grants No. CNS-0520033, CNS-0834585, and CNS-0831753M.

[11] Rongxing Lu, Xiaodong Lin, Haojin Zhu, and Xuemin (Sherman) Shen "A New VANET-based Smart Parking Scheme for Large Parking Lots" This full text paper was peer reviewed at the dirction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2009 proceedings.

[12] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments.Security Services for Applications and Management Messages,IEEE Std. 1609.2-2006, 2006.

[13] Y. Jiang, M. Shi, and X. S. Shen, "BAT: a robust signature scheme for vehicular networks using binary authentication tree," IEEE Trans.Wireless Commun., vol. 8, no. 4, pp. 1974–1983, 2009.

[14] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 88-95, 2008.

[15] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: a secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh.Technol., vol. 56, no. 6, pp. 3442–3456, 2007.

[16] T. Leinm¨uller, C. Mai¨ofer, E. Schoch, and F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification,"2006 VANET.